Security of decoy-state quantum key distribution with inexactly controlled source

Xiang-Bin Wang,[1,2] Cheng-Zhi Peng,[1,3] Jun Zhang,[3] and Jian-Wei Pan[1,3,4]

[1]*Department of Physics, Tsinghua University, Beijing 100084, China*
[2]*Imai-Project, ERATO-SORST, JST, Daini Hongo White Building, 201, 5-28-3, Hongo, Bunkyo, Tokyo 113-0033, Japan Department of Physics, Tsinghua University, Beijing 100084, China*
[3]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*
[4]*Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg, Germany*

The existing theory of decoy-state quantum cryptography assumes the counting rates of the same state from different sources to be the same, given whatever channel. This is correct if the intensity of each individual pulse is controlled exactly. We show by an explicit example that the assumption is in general incorrect if the source is inexactly controlled and the error pattern is known to Eve. We then further develop the theory of decoy-state method so that it is unconditionally secure given whatever error pattern provided that the error is not too large and the bounds of errors are known. Our result is not only limitted to the coherent states. It allpies to all source states satisfying Eq.(17).

PACS numbers: 03.67.Dd, 42.81.Gs, 03.67.Hk

Introduction.— Most of the existing set-ups of quantum key distribution (QKD)[1, 2, 3, 4, 5] use imperfect single-photon source. Such an implementation in principle suffers from the photon-number-splitting attack [6, 7]. The decoy-state method [8, 9, 10, 11, 12] and some other methods [13, 14, 15] can be used for unconditionally secure QKD even Alice only uses an imperfect source[6, 7].

The separate theoretical results of ILM-GLLP [5] shows that a secure final key can be distilled even though an imperfect source is used in the protocol, if one knows the lower bound of the fraction of those raw bits generated by single-photon pulses from Alice. The decoy-state method is to verify such a bound faithfully and efficiently. Recently, a number of experiments on decoy-state QKD have been done [16, 17]. However, the existing decoy-state theory assumes the perfect control of light intensity. This is an impossible task for any real set-up in practice. Here we study the decoy-state method with intensity errors and we conclude that after revising, the decoy-state method is still secure and efficient. Our result immediately applies to all existing experimental results.

Existing theory .— Given a class of N_x pulses, after Alice sends them out to Bob, if Bob observes n_x counts at his side, the *counting rate* for pulses in this class is

$$s_x = n_x/N_x. \tag{1}$$

Proposition 1: If class X is divided into l subclasses and any pulse in X belongs to only one subclass and the fraction of pulses in each subclasses are $a_0, a_1 \cdots, a_l$, then the counting rate of class X is $S_X = \sum_{k=0}^{l} a_k s_k$ and s_k is the counting rate of the kth subclass.

Proposition 2. The counting rate of pulses from class y must be equal to that of class y' if: 1) each class contains sufficiently large number of pulses; 2) pulses of each class are independent and identical; 3) the density operator of a pulse from class y is equal to that of class y', 4) pulses of y and y' are randomly mixed.

Alice has 3 different sources $Y_0, Y_\mu, Y_{\mu'}$ which can produce states of $\rho_0 = |0\rangle\langle 0|, \rho_\mu, \rho_{\mu'}$ only. Suppose

$$\rho_\mu = \sum_{k=0} a_k |k\rangle\langle k|;\ \rho_{\mu'} = \sum_{k=0} a'_k |k\rangle\langle k| \tag{2}$$

and we request the following constraints for all $n > 2$:

$$\frac{a'_k}{a_k} > \frac{a'_2}{a_2}. \tag{3}$$

Here the states are subscribed by μ and μ' because the diagonal states are actually determined by the intensity μ or μ'. For example, a coherent state of intensity q with phase randomization is

$$\rho_\mu = \sum_{k=0}^{\infty} \frac{\mu^k e^{-\mu}}{k!} |k\rangle\langle k|. \tag{4}$$

If Alice uses coherent states of intensity 0, μ, and μ' for source Y_0, Y_μ and $Y_{\mu'}$ in the protocol, the state parameters are $a_k = \frac{\mu^k e^{-\mu}}{k!}$, $a'_k = \frac{\mu'^k e^{-\mu'}}{k!}$.

We regard the pulses from each source as a *class*, i.e.class Y_0 for intensity 0, class Y_μ for intensity μ' and class $Y_{\mu'}$ for intensity μ'. We shall also call the pulses in class Y_μ, $Y_{\mu'}$ the *decoy pulses* and the *signal pulses*, respectively for simplicity. We regard those decoy or signal pulses containing k photons as (sub-)class y_k or y'_k. We also use the term sub-source for sub-class.

Proposition 1 leads to the following relation,

$$S_\mu = \sum_{k=0}^{\infty} a_k s_k = a_0 s_0 + a_1 s_1 + \lambda \tag{5}$$

and $\lambda = \sum_{k=2}^{\infty} a_k s_k$, S_μ is the total counting rate of all decoy pulses, s_k is the counting rate of pulses in class y_k. Also, we have

$$S_{\mu'} = \sum_{k=0}^{\infty} a'_k s'_k \tag{6}$$

and $S_{\mu'}$, s_k' are the counting rates of all signal pulses and class y_k', respectively[10]. In the protocol, Alice chooses each source randomly in producing each pulse for Bob. If each source always produces the assumed state exactly, pulses from sub-sources y_0, y_0', Y_0 are randomly mixed, and so are classes y_k, y_k'. According to Proposition 2,

$$s_0 = s_0' = S_0,\ s_k = s_k' \tag{7}$$

where S_0 is the counting rate of class Y_0. Also, using the assumed condition in Eq.(3), we can simplify Eq.(6) as

$$S_{\mu'} = \sum_{k=0}^{\infty} a_k' s_k \geq a_0' s_0 + a_1' s_1 + \frac{a_2'}{a_2}\lambda. \tag{8}$$

According to the definition of counting rate, $S_0, S_\mu, S_{\mu'}$ can be observed directly in the protocol. Since there are only two unknown variables (s_1, λ) for two constraints in Eq.(5) and Eq.(8), the lower bound value of s_1 can be verified by solving these joint constraints.

$$s_1 \geq \frac{a_2'(S_\mu - a_0 s_0) - a_2(S_{\mu'} - a_0' s_0)}{a_2' a_1 - a_1' a_2}. \tag{9}$$

Given this, one can calculate the final key rate by[5, 11]

$$R = \Delta_1'[1 - H(t_1)] - H(t) \tag{10}$$

where $\Delta_1' = \frac{a_1 s_1}{S_{\mu'}}$ is the fraction of single-photon counts among the raw bits due to signal pulses and t_1, t are the QBER for single-photon pulses and the QBER for all signal pulses. This is the result the decoy-state method with whatever diagonal source-state, including the coherent state, thermal state, heralded single-photon state, and so on with the condition of Eq.(3) and exactly controlled source.

The consequence of correlated intensity error.—The existing theory assumes that the parameters for state of *each individual decoy pulses and signal pulses* keep to be constant. In practice, these parameters cannot be constant for all pulses[19, 20]. If the parameter errors are independent, then we can [19] use the averaged state for each source to verify the lower bound of s_1 by Eq.(9). However, the issue becomes more complicated in the most general situation when there are correlated intensity errors. As shown explicitly below, in such a case, the average-state method fails and we have to consider the instantaneous intensity of each individual pulses.

There can be correlated intensity errors which are not known to Alice and Bob but is known to Eve. (This situation is more realistic if one uses the decoy-state plug-and-play protocol[21], where Eve. can actually prepare the error pattern). Consider a specific example. In the whole protocol, the pulses are divided into M blocks. Each block contains N/M pulses and $N = N_0 + N_\mu + N_{\mu'}$, where $N_0, N_\mu, N_{\mu'}$ are number of pulses from source $Y_0, Y_\mu, Y_{\mu'}$, N is the total number of pulses. The state of each individual pulse from source $Y_0, Y_{\mu'}$ are always controlled exactly. But there are errors for the state of pulses from source Y_μ (decoy pulse). Say, in half of those M blocks, state for every decoy pulse is actually vacuum (we name any of such blocks as block D_0). In the other half of blocks, the intensity of each decoy pulse is twice of the assumed value, i.e., 2μ, and μ is the value for the assumed intensity that Alice *wants* to use for each decoy pulse. We name these blocks as block D_2. Note that either block D_0 or block D_2 consists of three classes, $Y_0, Y_\mu, Y_{\mu'}$. Eve. knows such type of error pattern but Alice does not know it. We shall assume $\mu = 0.2$ and $\mu' = 0.6$ in the protocol. Actually, by watching the averaged photon number of each block, Eve can know exactly the intensity of decoy pulses in each block, i.e., 0 or $2\mu = 0.4$, provided that N/M is not so small.

Here is Eve's scheme using **time-dependent channel**: she blocks all pulses from block D_0, and she produces a linear channel of transmittance η_e to attenuate each pulse from block D_2. Straightly, the actual counting rate for the sub-source y_1 is $s_1 = \frac{2\eta_e \mu e^{-2\mu}}{2\mu e^{-2\mu}} = \eta_e$ and the actual counting rate for sub-source y_1' is

$$s_1' = \frac{1}{2}\frac{\eta_e \mu' e^{-\mu'}}{\mu' e^{-\mu'}} = \eta_e/2. \tag{11}$$

Obviously, $s_1 \neq s_1'$. Similarly, we can also show that $s_k \neq s_k'$. This shows, given the correlated error which is known to Eve, Eve can treat the pulses from sub-sources y_k and y_k' *differently*! Proposition 2 of the existing decoy-state theory can not be used anymore. Given the correlated intensity error, pulses from sub-source y_k and y_k' are actually *not randomly mixed*: in some blocks, the number of $k-$photon decoy pulses are larger than that of other blocks.

If one disregards the fact that Proposition 2 does not hold now and go ahead to use Eq.(9) with the *averaged state* for the decoy pulse, the protocol will be insecure because the calculated value of the single-photon counting rate by the existing theory will be larger than the true value. For simplicity, we assume $S_0 = 0$. Given the Eve's scheme above, Alice and Bob will find

$$S_\mu = \frac{1 - e^{-2\eta_e \mu}}{2} \approx 0.2\eta_e;\ S_{\mu'} = \frac{1 - e^{-\eta_e \mu'}}{2} \approx 0.3\eta_e \tag{12}$$

If we go ahead to assume $s_k = s_k'$ and blindly use Eq.(9), the counting rate of sub-source y_1' can be obtained by replacing a_i with the $0.4^k e^{-0.4}/k!/2$ there. The result for the counting rate of single-photon pulses by Eq.(9) is

$$s_1 = s_1' \geq 2.65336\eta_e \tag{13}$$

which is larger than the real value $\eta_e/2$ as shown Eq.(11). This means, *the value of counting rate for single-photon from signal pulses verified by the protocol would be larger than the true value* and hence the protocol is insecure.

A more realistic case[8] that in certain blocks, intensities of all pulses are a bit higher and in other blocks intensities of all pulses are a bit lower than the assumed values, it is also found that $s_1 \neq s_1'$ therefore existing decoy state theory cannot be used blindly.

Remark on proposition 2.— The above study has clearly shown that, if there are correlated intensity errors of light intensity, Proposition 2 cannot be blindly used because here y_1 and y_1' are *not* randomly mixed and the result is insecure given the time-dependent Eve's channel.

Our solution.— In the actual protocol, each pulse sent from Alice is randomly chosen from one of 3 sources $\{Y_0, Y_\mu, Y_{\mu'}\}$ with probability $p_0, p_\mu, p_{\mu'}$ ($p_0 + p_\mu + p_{\mu'} = 1$). For simplicity, we assume that every pulse in class Y_0 is exactly in vacuum state. But each single shot of pulse in classes $Y_\mu, Y_{\mu'}$ can be in a state slightly different from the expected one. We assume at time i Alice actually produces

$$\rho_{\mu i} = \sum a_{ki}|k\rangle\langle k| \quad (14)$$

or

$$\rho_{\mu' i} = \sum a'_{ki}|k\rangle\langle k| \quad (15)$$

instead of ρ_μ or $\rho_{\mu'}$ as defined in Eq.(2), where the parameters of each $|k\rangle\langle k|$ are constant. If Alice uses coherent states, the time-dependent parameters a_{ki}, a'_{ki} are determined by the time-dependent intensities by $a_{ki} = \frac{\mu_i^k e^{-\mu}}{k!}$, $a'_{ki} = \frac{\mu_i'^k e^{-\mu_i'}}{k!}$, and μ_i(or μ_i') is the instantaneous intensity of the i'th pulse (decoy signal pulse). Lets first consider a virtual protocol, **Protocol 1**: At each time i in sending a pulse to Bob, Alice produces a two-pulse (pulse A and pulse B) bipartite state

$$\rho_i^2 = p_0|z_0\rangle\langle z_0|\otimes|0\rangle\langle 0| + p_\mu|z_1\rangle\langle z_1|\otimes\rho_{\mu i} + p_{\mu'}|z_2\rangle\langle z_2|\otimes\rho_{\mu_i'} \quad (16)$$

Here the first subspace is for pulse A and the second subspace is for pulse B; i runs from 1 to N, the total number of pulses transmitted to Bob. States $\{|z_x\rangle\}$ are orthogonal to each other for different x ($x = 0, 1, 2$). Alice keeps pulse A and sends out pulse B to Bob. After Bob completes the detection, Alice measures pulse A. The outcome of $|z_0\rangle, |z_1\rangle$ or $|z_2\rangle$ of pulse A corresponds to class Y_0, Y_μ or $Y_{\mu'}$ for pulse B. Asymptotically, the number of pulses in theses classes should be $N_0 = p_0 N$, $N_\mu = p_\mu N$, $N_{\mu'} = p_{\mu'} N$. We use notation a_k^L, a_k^U for lower bound and upper bound of $\{a_{ki}|i = 0, 1 \cdots N\}$, $a_k'^L, a_k'^U$ for lower bound and upper bound of $\{a'_{ki}|i = 0, 1, \cdots N\}$. Also, we need

$$\frac{a_k'^L}{a_k^U} \geq \frac{a_2'^L}{a_2^U} > 1 \quad (17)$$

for all $k > 2$. In the protocol, Alice *could* have known the exact photon number in any pulse before sending it to Bob. We define those pulses containing k photons as class $\tilde{y}_k$, e.g., all the single-photon pulses make of class $\tilde{y}_1$. For clarity, we also define set $\{l_k\}$ ($k = 0, 1, 2 \cdots$): for the ith pulse (i from 1 to N), if the pulse contains k photons, then $i \in l_k$. Since Alice could have known the photon number in each pulse, any i must belong to only one l_k. Asymptotically, there should be $N_k = \sum_1^N (p_\mu a_{ki} + p_{\mu'} a'_{ki})$ pulses (elements) in class (set) $\tilde{y}_k$ (l_k) for any $k > 0$ and there are $N_0 = \sum_{i=1}^N (p_0 + a_{0i}p_\mu + a'_{0i}p_{\mu'})$ pulses (elements) in class (set) $\tilde{y}_0$ (l_0). Also, each individual pulse can only belong to one class from $\{\tilde{y}_k|k = 0, 1, \cdots\}$. Most generally, we assume the *instantaneous* transmittance of the i'th pulse to be η_i (i from 1 to N), which should be either 0 or 1. If the pulse causes no count at Bob's side, the instantaneous counting rate for that pulse is 0, otherwise it is 1. Given any photon number state $|k\rangle\langle k|$, it can be from both class Y_μ and class $Y_{\mu'}$. Asymptotically, the numbers of counts caused by decoy pulses (pulses from class Y_μ), signal pulses and pulses in class Y_0 are

$$n_\mu = \sum_{i\in l_0} p_\mu a_{0i} d_i + \sum_{k=1}^{\infty}\sum_{i\in l_k} p_\mu a_{ki} d_i, \quad (18)$$

$$n_{\mu'} = \sum_{i\in l_0} p_{\mu'} a'_{0i} d_i + \sum_{k=1}^{\infty}\sum_{i\in l_k} p_{\mu'} a'_{ki} d_i \quad (19)$$

and

$$n(Y_0) = \sum_{i\in l_0} \frac{p_0}{p_0 + p_\mu a_{0i} + p_{\mu'} a'_{0i}} \eta_i, \quad (20)$$

respectively, where d_i is defined as

$$d_i = \frac{\eta_i}{p_\mu a_{0i} + p_{\mu'} a'_{0i} + p_0}; \text{ if } i \in l_0 \quad (21)$$

$$d_i = \frac{\eta_i}{p_\mu a_{ki} + p_{\mu'} a'_{ki}}; \text{ if } i \in l_k,\ k \geq 1 \quad (22)$$

The values of $n_\mu, n_{\mu'}$ and $n(Y_0)$ can be directly observed in the protocol, therefore are regarded as known parameters. Based on Eq.(20), we have the following inequality:

$$\sum_{i\in l_0} p_\mu a_{0i} d_i \leq \frac{p_\mu a_0^U n(Y_0)}{p_0} = p_\mu a_0^U S_0 N, \quad (23)$$

$$p_{\mu'} a'_{0i} d_i \geq \frac{p_{\mu'} a_0'^L n(Y_0)}{p_0} = p_{\mu'} a_0'^L S_0 N \quad (24)$$

and $S_0 = \frac{n(Y_0)}{p_0 N}$, the counting rate of class Y_0, which is observed in the protocol itself. Given bounded values for parameters $\{a_{ki}, a'_{ki}\}$, we have

$$n_\mu \leq p_\mu a_0^U S_0 N + p_\mu a_1^U \sum_{i\in l_1} d_i + p_\mu \sum_{k=2}^{\infty} a_k^U (\sum_{i\in l_k} d_i) \quad (25)$$

TABLE I: Secure key rate (R) vs different values of intensity error upper bound (δ_M) using the experimental data in the case of 50 km [17]. The experiment lasts for 1481.2 seconds with the repetition rate 4 MHz. We have observed $S_{\mu'} = 3.817 \times 10^{-4}, S_\mu = 1.548 \times 10^{-4}, S_0 = 2.609 \times 10^{-5}$ and the quantum bit error rates (QBER) for signal states and decoy states are $4.247\%, 8.379\%$ respectively.

δ_M	5%	4%	3%	2%	1%	0
R (Hz)	70.8	84.3	97.6	110.7	123.6	136.3

and

$$n_{\mu'} \geq p_{\mu'} a_0'^L S_0 N + p_{\mu'} a_1'^L \sum_{i \in l_1} d_i + p_{\mu'} \sum_{k=2}^{\infty} a_k'^L (\sum_{i \in l_k} d_i). \tag{26}$$

Using the assumed conditions given in Eq.(17) we can solve the above simultaneous constraints and obtain

$$\frac{1}{N} \sum_{i \in l_1} d_i \geq \frac{a_2'^L S_\mu - a_2^U S_{\mu'} + a_0'^L a_2^U S_0 - a_0^U a_2'^L S_0}{a_2'^L a_1^U - a_1'^L a_2^U} \tag{27}$$

where $S_\mu = \frac{n_\mu}{p_\mu N} = \frac{n_\mu}{N_\mu}$, $S_{\mu'} = \frac{n_{\mu'}}{N_{\mu'}}$. The fraction of single-photon counts among those counts caused by signal pulses is $\frac{\sum_{i \in l_1} a_{1i}' d_i}{p_{\mu'} N S_{\mu'}}$, which is lower bounded by

$$\Delta_1' \geq \frac{a_1'^L (a_2'^L S_\mu - a_2^U S_{\mu'} + a_0'^L a_2^U S_0 - a_0^U a_2'^L S_0)}{S_{\mu'} (a_2'^L a_1^U - a_1'^L a_2^U)} \tag{28}$$

and the fraction of single-photon counts of decoy pulses is lower bounded by

$$\Delta_1 \geq \frac{a_1^L (a_2'^L S_\mu - a_2^U S_{\mu'} + a_0'^L a_2^U S_0 - a_0^U a_2'^L S_0)}{S_\mu (a_2'^L a_1^U - a_1'^L a_2^U)} \tag{29}$$

For coherent states, if the intensity is bounded by $[\mu^L, \mu^U]$ for decoy pulses and $[\mu'^L, \mu'^U]$ for signal pulses then

$$a_k^X = (\mu^X)^k e^{-\mu^X}/k!, \; a_k'^X = (\mu'^X)^k e^{-\mu'^X}/k! \tag{30}$$

with $X = L, U$ and $k = 1, 2$. Therefore, one can calculate the final key rate by Eq.(10) now, if the bound values of intensity errors are known. The asymptotic result using the experimental data of QKD distance of 50 kilometers calculated by our formula is listed in table I.

The results above are for the virtual protocol where Alice uses the bipartite state of Eq.(16). Obviously Alice can choose to measure all A-pulses of each bipartite state in the very beginning and the virtual protocol is reduced to the normal protocol in practice, where the bipartite state is not necessary.

Application in the Plug-and-Play protocol.— As shown by Gisin et al[21], combining with the decoy-state method, the plug-and-play protocol can be unconditionally secure. There, Alice receives strong pulses from Bob and she needs to guarantee the exact intensity of the pulse sending to Bob. It is not difficult to monitor the intensity, but difficult to *control* the intensity. Our theory here can help to save the difficult feed-back intensity control: Alice monitors the intensities, discards those pulses whose intensity error is too large, and then use our theory with the known bound bound of intensity errors.

Concluding remark: In summary, we have shown the the unconditional security of decoy-state method given what-ever error patern of the source, provided that the parameters diagonal state of the source satisfy Eq.(17) and the bound values of each parameters in the state is known. Our result here applies to whatever distribution of source state that satisfies Eq.(17). Our result also answers clearly the often asked question "What happens if the state of Laser beam is not exactly in the assumed distribution ?". Here we don't need exact information about the source state, we only need the bound values for parameters $a_1, a_2.1_1', a_2'$ and Eq.(17).

Acknowledgement: This work was supported in part by the National Basic Research Program of China grant No. 2007CB907900 and 2007CB807901, NSFC grant No. 60725416 and China Hi-Tech program grant No. 2006AA01Z420.

[1] C.H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing (IEEE, New York, 1984)*, pp. 175-179.

[2] D. Bruss, Phys. Rev. Lett, 81, 3018(1998).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[4] M. Dusek, N. Lütkenhaus, M. Hendrych, in *Progress in Optics VVVX*, edited by E. Wolf (Elsevier, 2006).

[5] H. Inamori, N. Lütkenhaus, D. Mayers, quant-ph/0107017; D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[6] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H.P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).

[7] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[8] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, *Physics Reports* 448, 1(2007)

[9] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[10] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).

[11] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[12] J.W. Harrington *et al.*, quant-ph/0503002.

[13] R. Ursin *et al.*, quant-ph/0607182.

[14] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Phys. Rev. Lett. 92, 057901 (2004); C. Branciard, N. Gisin, B. Kraus, V. Scarani, Phys. Rev. A 72, 032301 (2005).

[15] M. Koashi, Phys. Rev. Lett., 93, 120501(2004); K. Tamaki, N. Lükenhaus, M. Loashi, J. Batuwantudawe, quant-ph/0608082

[16] Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006); Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, quant-ph/0601168.

[17] Cheng-Zhi Peng *et al.* Phys. Rev. Lett. 98, 010505 (2007); D. Rosenberg em et al., *Phys. Rev. Lett.* 98, 010503 (2007), T. Schmitt-Manderbach *et al.*, *Phys. Rev. Lett.* 98, 010504 (2007).

[18] Z.-L. Yuan, A. W. Sharpe, and A. J. Shields, *Appl. Phys. Lett.* 90, 011118 (2007).

[19] X.-B. Wang, *Phys. Rev.* A75, 012301(2007)

[20] X.-B. Wang, C.-Z. Peng and J.-W. Pan, *Appl. Phys. Let.* 90, 031110(2007)

[21] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A 73, 022320(2006).